REMARKS

Prior to entry of this paper, Claims 1-24 were pending. In this paper, Claims 1 and 10-15 are amended; no claims are cancelled nor added. Claims 1-24 are currently pending. No new matter is added by way of this amendment. For at least the following reasons, Applicant respectfully submits that each of the presently pending claims is in condition for allowance.

Claim Rejections – 35 U.S.C. § 102

Claims 1-24 are rejected under 35 U.S.C. 102 (e) as being anticipated by Goldstein et al (US 6,957,335). Applicant respectfully traverses this rejection.

Applicant holds that Goldstein does not teach or suggest "enabling at least the encrypted string to be locally decrypted *at the user node,*" as recited in at least Claim 1. Instead, Goldstein teaches that "authentication documents are encrypted in a form that an *intended merchant* can decrypt" and that "the authentication document is signed by the guarantor and then encrypted with the *public key of the recipient merchant.*" Emphasis added; see Goldstein, column 2, lines 66-67; column 3, lines 56-58. Goldstein also discloses alternatively encrypting the authentication document using a symmetric encryption algorithm and a key *shared between at guarantor site 30 and merchant site 40.* Emphasis added; see Goldstein, column 6, lines 39-42. Thus, Goldstein's decryption key (either the private key of the merchant or the symmetric key) is available to the merchant and not the end user. Goldstein does not disclose a mechanism for enabling the encrypted authentication document to be locally decrypted at the user node. In fact to do so would render Goldstein's authentication document unsatisfactory for its intended purpose, which is to provide a "means to validate a user's identity and/or to provide authorization/validation of a specific transaction." Specifically, Goldstein provides a "trusted third-party authentication protocol," with a "guarantor" that authenticates users. See Goldstein, column 2, lines 46-53, and lines 55-57. To allow the Goldstein authentication document to be decrypted by the user would make the authentication document available to the end user for possible tampering. Thus, Goldstein's "trusted third-party authentication protocol" for authenticating the 'end user' through a guarantor and not at the end user itself would be destroyed if the end user could access and/or modify the

unencrypted authentication document. See Goldstein's Abstract. Again, unlike Goldstein, the user node of Claim 1 from the present application allows interacting with the locally decrypted string. Therefore, *Goldstein actually teaches away* from enabling the decryption to occur locally at the end user node as well as interacting with that locally decrypted string, as recited in at least Claim 1. Since Goldstein does not teach every limitation of at least Claim 1, the Applicant respectfully requests withdrawal of the outstanding rejection.

The Applicant points out that in this response, Claim 1 was amended to explicitly recite enabling at least the encrypted string to be locally decrypted "to allow interacting with the decrypted string" at the user node, whereas the prior language implied this limitation. As such, this amendment is not intended to narrow Claim 1 to overcome the prior art rejection discussed above, because it merely makes explicit that which was implicit. Accordingly, the scope of the equivalents afforded to the amended portion of Claim 1 should remain the same as it was prior to this amendment.

Furthermore, the Applicant holds that Goldstein does not teach or suggest, "concatenating data from a plurality of fields ... into a string," as recited in at least Claim 1. Instead, Goldstein merely teaches "encrypting the authentication document." See Goldstein, column 2, lines 55-57; column 3, lines 13-14. While Goldstein does describe the authentication document to include, in one form, the user's name, payment information, a guarantee number, a time limit, possibly a user's preferred delivery address, or a vast array of information, nowhere does Goldstein teach or suggest that this authentication document is a string created by concatenating data from a plurality of fields of a requested web page. See Goldstein, column 5, lines 60 through column 6, lines 10. In fact, Goldstein does not appear to teach or suggest any string created by concatenating data, let alone as claimed, from a plurality of fields of a requested web page. Thus, Goldstein's authentication document is not the same as the Applicant's string as claimed in at least Claim 1. Therefore, for at least this reason, Goldstein's encryption of the authentication document does not anticipate nor render obvious at least this limitation of Claim 1. Because Claim 1 is not anticipated by Goldstein, it should be allowed to issue.

Independent Claims 10 and 16 include similar, albeit different limitations as recited above for Claim 1. For example, Claim 10 recites, in part, locally decrypting the encrypted string. Claim 16 recites, in part, concatenating data into a string and enabling the encrypted string to be locally decrypted at the user node. Thus, for at least the same reasons as noted above, Goldstein does not anticipate nor render obvious Claim 10 or 16, and they too should be allowed to issue.

Further, Claim 10 recites, in part, distributing a plurality of portions of the decrypted string to the plurality of blank fields in the form. As described by Goldstein, the authentication document is forwarded from the user to the merchant for validation. See Goldstein, column 6, lines 33-42. Nowhere does Goldstein appear to teach or suggest that the authentication document is divided into a plurality of portions and distributed to the plurality of blank fields in a form, as recited by at least Claim 10. Instead, Goldstein merely discloses that the document is used by the merchant for validation. Therefore, Claim 10 is not anticipated nor rendered obvious by Goldstein and should also be allowed to issue.

As recited in Claim 7, Applicant holds that Goldstein does not teach the login data forming a basis for a key used to encrypt the string. Regarding login information, Goldstein merely teaches that "the user logs on to the guarantor's site and is prompted for a user name and a password for authentication purposes.... The guarantor generates an authentication documents [which] is signed by the guarantor and then encrypted with the *public key of the recipient merchant*." See Goldstein, column 3, lines 40-58. Goldstein explicitly states that the public key is associated with the *merchant*. However, nowhere does Goldstein disclose or suggest that the public/private key pair is generated using the *user's* login information. Therefore, for at least this reason, Goldstein's merchant's public key (or symmetric key) does not anticipate nor render obvious the user's login data to form the basis for a key to encrypt the string. Thus, Claim 7 is not anticipated nor rendered obvious by Goldstein and should be allowed to issue.

In addition, Claims 2-9 depend from Claim 1; Claims 11-15 depend from Claim 10; and Claims 17-24 depend from Claim 16. Therefore, for at least the same reasons as their respective

independent claims, each of the dependent claims is also allowable. Thus, Applicant respectfully submits that Claims 1-24 are in condition for allowance, and should be allowed to issue.

CONCLUSION

It is respectfully submitted that each of the presently pending claims (Claims 1-24) are in condition for allowance and notification to that effect is requested. Examiner is invited to contact the Applicant's representative at the below-listed telephone number if it is believed that the prosecution of this application may be assisted thereby. Although only certain arguments regarding patentability are set forth herein, there may be other arguments and reasons why the claimed invention is patentable. Applicant reserves the right to raise these arguments in the future.

Dated: February 27, 2007

Respectfully submitted,

By _____
Jamie L. Wiegand
Registration No.: 52,361
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(206) 262-8915
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant